FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE IT00147
NETWORK INFORMATION SECURITY

CAMPUS APK

EXAM NOVEMBER 2014

DATE: 2014/11/10 **TIME:** 08:30 – 10:30

ASSESSORS(S) Prof M Coetzee

EXTERNAL MODERATOR Mrs L Drevin (NWU)

DURATION: 2 HOURS **MARKS:** 80

THIS PAPER CONSISTS OF 3 PAGES INCLUDING THE COVER PAGE

INSTRUCTIONS:

1. Answer **ALL** the questions.
2. Write neatly and legibly.
3. Read the questions thoroughly.
4. Ensure that all questions are clearly marked on the answer sheet.

REQUIREMENTS: NONE

QUESTION 1

RC4 was a good choice for WEP. Evaluate this statement critically.

[10]

QUESTION 2

By using the 802.1X authentication framework, the evil twin attack can be prevented.

Discuss this statement and motivate if you agree or disagree by:

a) Explaining what 802.1X is and how it works. (10)
b) Now stating if you agree or disagree if the 802.1X authentication framework can or cannot prevent an evil twin attack. Explain your choice. (5)

[15]

QUESTION 3

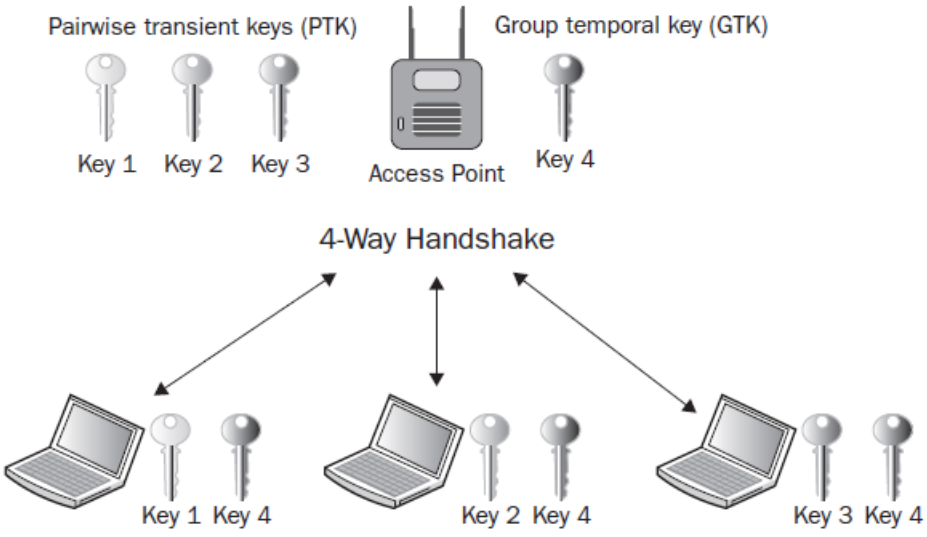
CCMP is the security protocol that was created as part of the 802.11i security amendment. CCMP uses CCM that combines CTR for data confidentiality and CBC-MAC for authentication and integrity.

a) Give the full acronym of CCMP. (2)
b) Explain what CCMP is. (7)
c) Discuss how it addresses confidentiality, authentication and integrity. (6)

[15]

QUESTION 4

Dynamic encryption keys can be generated as a by-product of the 802.1X/EAP process as mutual authentication is required to generate unique dynamic encryption keys.EAP protocols that utilize mutual authentication provide " seeding material " that can be used to generate encryption keys dynamically. This process results in an access point and laptops having a set of keys as shown in the diagram below.



Answer the following:

a) Name and describe all keys found in the process to create dynamic keys. (10)
b) Can Key 1 and Key 2 be the same key? Explain why you say so by fully motivating your answer. (3)
c) Is Key 4 the same on all nodes? Explain why you say so by fully motivating your answer. (3)

[15]

QUESTION 5

After mesh discovery with passive or active scanning, two neighbour mesh STAs within direct wireless communication with one another need to agree to establish a mesh peering to each other to be able to communicate directly with one another. A key concern for peering is security. As peering is a very flexible process, the risk exists that a rogue mesh station would peer with a valid mesh station, thus hijacking a legitimate MBSS's bandwidth or offering rogue connections to fake resources or the wired network. unfortunately, a limitation of 802.1X is AAA server reachability.

Name and discuss the peer to peer, mutual authentication process defined for 802.11s mesh networks.

[10]

QUESTION 6

The emergence of the Mobile Ad Hoc Networking (MANET) technology advocates self-organized wireless interconnection of communication devices that would either extend or operate in concert with the wired networking infrastructure or possibly, evolve to autonomous networks. In either case, the proliferation of MANET-based applications depends on a multitude of factors, with trustworthiness being one of the primary challenges to be met. Despite the existence of well-known security mechanisms, additional vulnerabilities and features pertinent to this new networking paradigm might render such traditional solutions inapplicable. In particular, the absence of a central authorization facility in an open and distributed communication environment is a major challenge, especially due to the need for cooperative network operation. In particular, in MANET, any node may compromise the routing protocol functionality by disrupting the route discovery process.

Discuss secure routing for Mobile Ad Hoc Networks (MANET).

[15]